BDTIC www.BDTIC.com/ATMEL

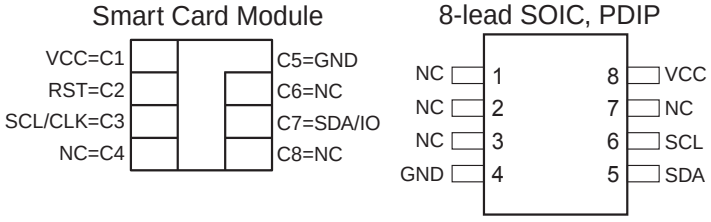
Features

- One of a Family of 9 Devices with User Memories from 1 Kbit to 256-Kbit
- 8-Kbit (1-Kbyte) EEPROM User Memory
  - Eight 128-byte (1-Kbit) Zones
  - Self-timed Write Cycle
  - Single Byte or 16-byte Page Write Mode
  - Programmable Access Rights for Each Zone
- 2-Kbit Configuration Zone
  - 37-byte OTP Area for User-defined Codes
  - 160-byte Area for User-defined Keys and Passwords
- High Security Features
  - 64-bit Mutual Authentication Protocol (Under License of ELVA)
  - Encrypted Checksum
  - Stream Encryption
  - Four Key Sets for Authentication and Encryption
  - Eight Sets of Two 24-bit Passwords
  - Anti-tearing Function
  - Voltage and Frequency Monitor
- Smart Card Features
  - ISO 7816 Class A (5V) or Class B (3V) Operation
  - ISO 7816-3 Asynchronous T = 0 Protocol (Gemplus® Patent)
  - Multiple Zones, Key Sets and Passwords for Multi-application Use
  - Synchronous 2-wire Serial Interface for Faster Device Initialization
  - Programmable 8-byte Answer-To-Reset Register
  - ISO 7816-2 Compliant Modules
- Embedded Application Features
  - Low Voltage Operation: 2.7V to 5.5V
  - Secure Nonvolatile Storage for Sensitive System or User Information
  - 2-wire Serial Interface
  - 1.0 MHz Compatibility for Fast Operation
  - Standard 8-lead Plastic Packages, Green Compliant (exceeds RoHS)
  - Same Pinout as 2-wire Serial EEPROMs
- High Reliability
  - Endurance: 100,000 Cycles
  - Data Retention: 10 years
  - ESD Protection: 4,000V min

Table 1. Pin Configuration

Pad	Description	ISO Module Contact	Standard Package Pin
VCC	Supply Voltage	C1	8
GND	Ground	C5	4
SCL/CLK	Serial Clock Input	C3	6
SDA/IO	Serial Data Input/Output	C7	5
RST	Reset Input	C2	NC

Figure 1. Package Options



CryptoMemory® 8 Kbit

AT88SC0808C

Summary

Rev. 2024JS–SMEM–3/09

Note: This is a summary document. A complete document is available under NDA. For more information, please contact your local Atmel sales office.

Description

The AT88SC0808C member of the CryptoMemory® family is a high-performance secure memory providing 8 Kbits of user memory with advanced security and cryptographic features built in. The user memory is divided into 8 128-byte zones, each of which may be individually set with different security access rights or effectively combined together to provide space for 1 to 8 data files.

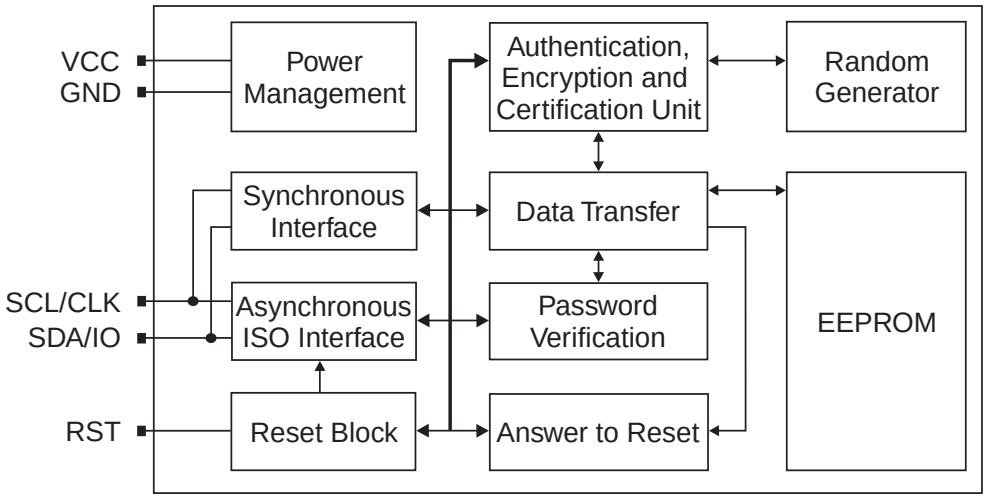
Smart Card Applications

The AT88SC0808C provides high security, low cost, and ease of implementation without the need for a microprocessor operating system. The embedded cryptographic engine provides for dynamic and symmetric mutual authentication between the device and host, as well as performing stream encryption for all data and passwords exchanged between the device and host. Up to four unique key sets may be used for these operations. The AT88SC0808C offers the ability to communicate with virtually any smart card reader using the asynchronous T = 0 protocol (Gemplus Patent) defined in ISO 7816-3.

Embedded Applications

Through dynamic and symmetric mutual authentication, data encryption, and the use of encrypted checksums, the AT88SC0808C provides a secure place for storage of sensitive information within a system. With its tamper detection circuits, this information remains safe even under attack. A 2-wire serial interface running at 1.0 MHz is used for fast and efficient communications with up to 15 devices that may be individually addressed. The AT88SC0808C is available in industry standard 8-lead packages with the same familiar pinout as 2-wire serial EEPROMs.

Figure 2. Block Diagram



Pin Descriptions

Supply Voltage (V_{CC}) The V_{CC} input is a 2.7V to 5.5V positive voltage supplied by the host.

Clock (SCL/CLK) In the asynchronous T = 0 protocol, the SCL/CLK input is used to provide the device with a carrier frequency *f*. The nominal length of one bit emitted on I/O is defined as an “elementary time unit” (ETU) and is equal to 372/*f*. When the synchronous protocol is used, the SCL/CLK input is used to positive edge clock data into the device and negative edge clock data out of the device.

Reset (RST) The AT88SC0808C provides an ISO 7816-3 compliant asynchronous answer to reset sequence. When the reset sequence is activated, the device will output the data programmed

into the 64-bit answer-to-reset register. An internal pull-up on the RST input pad allows the device to be used in synchronous mode without bonding RST. The AT88SC0808C does not support the synchronous answer-to-reset sequence.

Serial Data (SDA/IO)

The SDA pin is bidirectional for serial data transfer. This pin is open-drain driven and may be wired with any number of other open drain or open collector devices. An external pull-up resistor should be connected between SDA and V_{CC}. The value of this resistor and the system capacitance loading the SDA bus will determine the rise time of SDA. This rise time will determine the maximum frequency during read operations. Low value pull-up resistors will allow higher frequency operations while drawing higher average power. SDA/IO information applies to both asynchronous and synchronous protocols.

When the synchronous protocol is used, the SCL/CLK input is used to positive edge clock data into the device and negative edge clock data out of the device.

Table 2. DC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 5.5V, T_{AC} = -40°C to +85°C (unless otherwise noted)

Symbol	Parameter	Test Condition	Min	Typ	Max	Units
V_{CC}[2]	Supply Voltage		2.7		5.5	V
I_{CC}	Supply Current (V_{CC} = 5.5V)	Async READ at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Async WRITE at 3.57MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Synch READ at 1MHz			5	mA
I_{CC}	Supply Current (V_{CC} = 5.5V)	Synch WRITE at 1MHz			5	mA
I_{SB}	Standby Current (V_{CC} = 5.5V)	V_{IN} = V_{CC} or GND			100	uA
V_{IL}[1]	SDA/IO Input Low Threshold		0		V_{CC} x 0.2	V
V_{IL}[1]	SCL/CLK Input Low Threshold		0		V_{CC} x 0.2	V
V_{IL}[1]	RST Input Low Threshold		0		V_{CC} x 0.2	V
V_{IH}[1][2]	SDA/IO Input High Threshold		V_{CC} x 0.7		V_{CC}	V
V_{IH}[1][2]	SCL/CLK Input High Threshold		V_{CC} x 0.7		V_{CC}	V
V_{IH}[1][2]	RST Input High Threshold		V_{CC} x 0.7		V_{CC}	V
I_{IL}	SDA/IO Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	uA
I_{IL}	SCL/CLK Input Low Current	0 < V_{IL} < V_{CC} x 0.15			15	uA
I_{IL}	RST Input Low Current	0 < V_{IL} < V_{CC} x 0.15			50	uA
I_{IH}	SDA/IO Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			20	uA
I_{IH}	SCL/CLK Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			100	uA
I_{IH}	RST Input High Current	V_{CC} x 0.7 < V_{IH} < V_{CC}			150	uA
V_{OH}	SDA/IO Output High Voltage	20K ohm external pull-up	V_{CC} x 0.7		V_{CC}	V
V_{OL}	SDA/IO Output Low Voltage	I_{OL} = 1mA	0		V_{CC} x 0.15	V
I_{OH}	SDA/IO Output High Current	V_{OH}			20	uA

Notes: 1. V_{IL} min and V_{IH} max are reference only and are not tested.

2. To prevent Latch Up Conditions from occurring during Power Up of the AT88SCxxxxC, Vcc must be turned on before applying Vih. For Powering Down, Vih must be removed before turning vcc off.

Table 3. AC Characteristics

Applicable over recommended operating range from V_{CC} = +2.7 to 5.5V,

T_{AC} = -40°C to +85°C, CL = 30pF (unless otherwise noted)

Symbol	Parameter	Min	Max	Units
f_{CLK}	Async Clock Frequency (V_{CC} Range: +4.5 - 5.5V)	1	5	MHz
f_{CLK}	Async Clock Frequency (V_{CC} Range: +2.7 - 3.3V)	1	4	MHz
f_{CLK}	Synch Clock Frequency	0	1	MHz
	Clock Duty cycle	40	60	%
t_R	Rise Time - I/O, RST		1	uS
t_F	Fall Time - I/O, RST		1	uS
t_R	Rise Time - CLK		9% x period	uS
t_F	Fall Time - CLK		9% x period	uS
t_{AA}	Clock Low to Data Out Valid		35	nS
$t_{HD.STA}$	Start Hold Time	200		nS
$t_{SU.STA}$	Start Set-up Time	200		nS
$t_{HD.DAT}$	Data In Hold Time	10		nS
$t_{SU.DAT}$	Data In Set-up Time	100		nS
$t_{SU.STO}$	Stop Set-up Time	200		nS
t_{DH}	Data Out Hold Time	20		nS
t_{WR}	Write Cycle Time (at 25·C)		5	mS
t_{WR}	Write Cycle Time (-40° to +85°C)		7	mS

Device Operation For Synchronous Protocols

CLOCK and DATA TRANSITIONS: The SDA pin is normally pulled high with an external device. Data on the SDA pin may change only during SCL low time periods (see Figure 5 on page 5). Data changes during SCL high periods will indicate a start or stop condition as defined below.

START CONDITION: A high-to-low transition of SDA with SCL high is a start condition which must precede any other command (see Figure 6 on page 6).

STOP CONDITION: A low-to-high transition of SDA with SCL high is a stop condition. After a read sequence, the stop command will place the EEPROM in a standby power mode (see Figure 6 on page 6).

ACKNOWLEDGE: All addresses and data words are serially transmitted to and from the EEPROM in 8-bit words. The EEPROM sends a zero to acknowledge that it has received each word. This happens during the ninth clock cycle.

MEMORY RESET: After an interruption in protocol, power loss or system reset, any 2-wire part can be reset by following these steps:

1. Clock up to 9 cycles.
2. Look for SDA high in each cycle while SCL is high.
3. Create a start condition.

Figure 3. Bus Timing for 2 wire communications
SCL: Serial Clock, SDA: Serial Data I/O

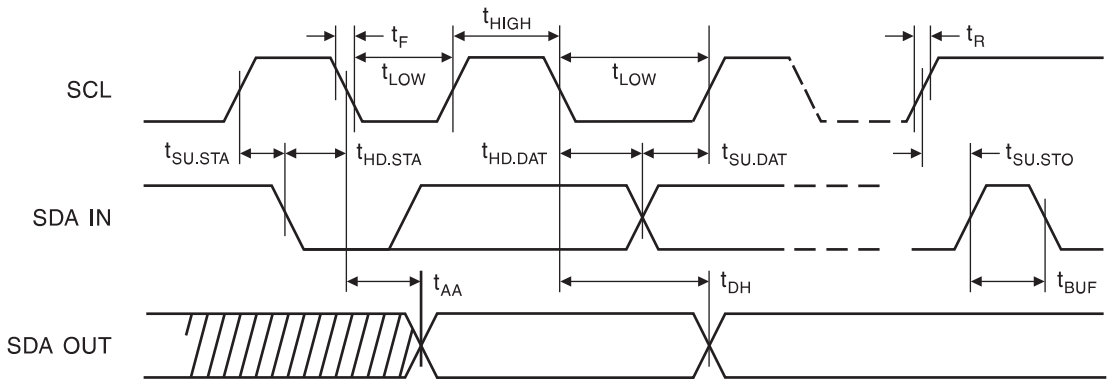
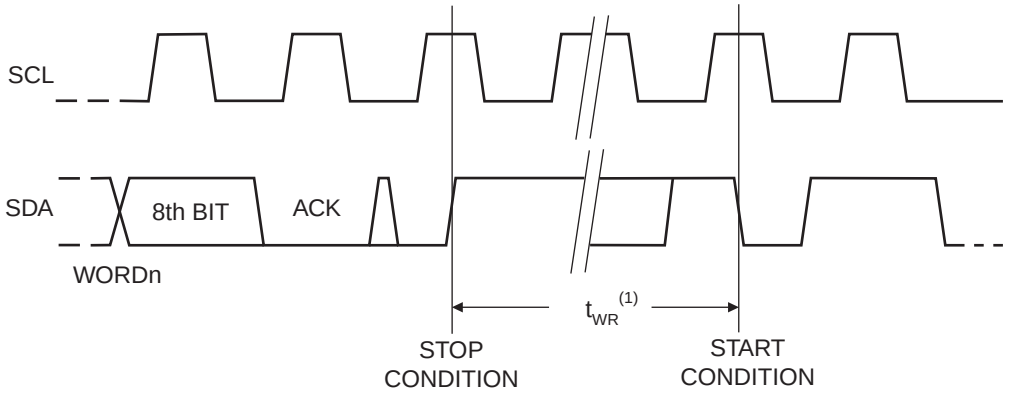


Figure 4. Write Cycle Timing:
SCL: Serial Clock, SDA: Serial Data I/O



Note: The write cycle time t_{WR} is the time from a valid stop condition of a write sequence to the end of the internal clear/write cycle.

Figure 5. Data Validity

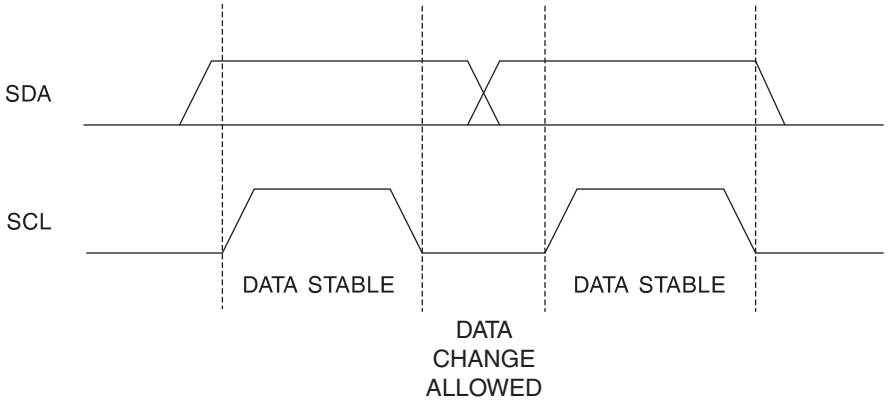


Figure 6. Start and Stop Definition

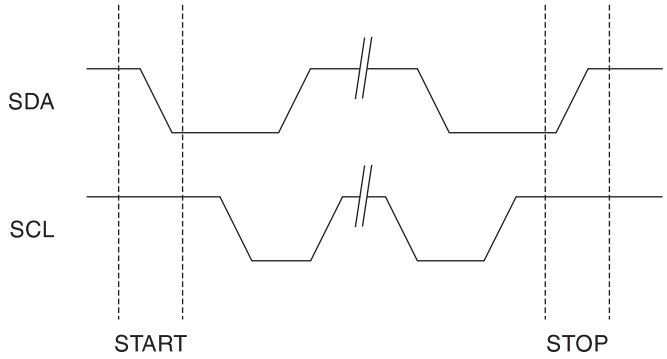
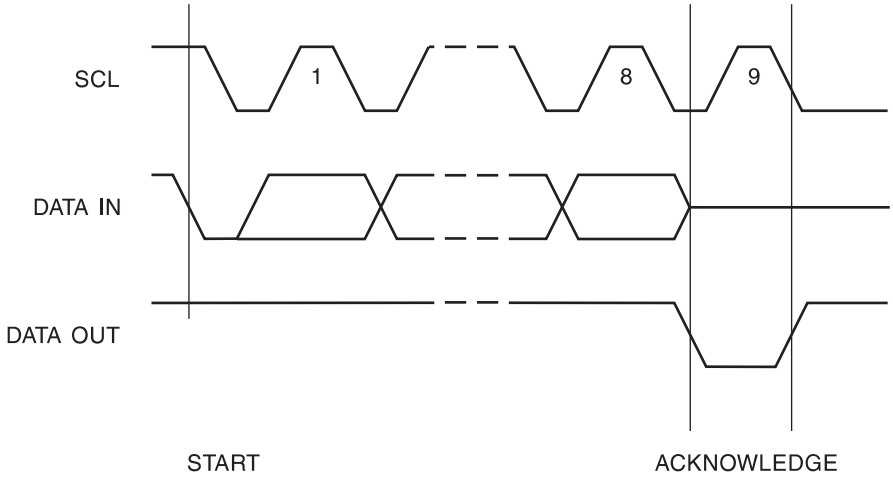


Figure 7. Output Acknowledge



Device Architecture

User Zones

The EEPROM user memory is divided into 8 zones of 1024 bits each. Multiple zones allow for different types of data or files to be stored in different zones. Access to the user zones is allowed only after security requirements have been met. These security requirements are defined by the user during the personalization of the device in the configuration memory. If the same security requirements are selected for multiple zones, then these zones may effectively be accessed as one larger zone.

Figure 8. User Zone

ZONE		$0	$1	$2	$3	$4	$5	$6	$7
User 0	$00								
	-	128 Bytes							
	-								
	$78								
User 1	$00								
-	-								
-									
-	-								
User 6	$78								
User 7	$00								
	-	128 Bytes							
	-								
	$78								

Control Logic

Access to the user zones occurs only through the control logic built into the device. This logic is configurable through access registers, key registers and keys programmed into the configuration memory during device personalization. Also implemented in the control logic is a cryptographic engine for performing the various higher-level security functions of the device.

Configuration Memory

The configuration memory consists of 2048 bits of EEPROM memory used for storing passwords, keys and codes and defining security levels to be used for each user zone. Access rights to the configuration memory are defined in the control logic and may not be altered by the user.

Figure 9. Configuration Memory

	$0	$1	$2	$3	$4	$5	$6	$7	
$00	Answer To Reset								**Identification**
$08	Fab Code		MTZ		Card Manufacturer Code				
$10	Lot History Code								**Read Only**
$18	DCR	Identification Number Nc							**Access Control**
$20	AR0	PR0	AR1	PR1	AR2	PR2	AR3	PR3	
$28	AR4	PR4	AR5	PR5	AR6	PR6	AR7	PR7	
$30	Reserved								
$38									
$40	Issuer Code								
$48									
$50	For Authentication and Encryption use								**Cryptography**
$58									
$60									
$68									
$70									
$78									
$80									
$88									
$90	For Authentication and Encryption use								**Secret**
$98									
$A0									
$A8									
$B0	PAC	Write 0			PAC	Read 0			**Password**
$B8	PAC	Write 1			PAC	Read 1			
$C0	PAC	Write 2			PAC	Read 2			
$C8	PAC	Write 3			PAC	Read 3			
$D0	PAC	Write 4			PAC	Read 4			
$D8	PAC	Write 5			PAC	Read 5			
$E0	PAC	Write 6			PAC	Read 6			
$E8	PAC	Write 7			PAC	Read 7			
$F0	Reserved								**Forbidden**
$F8									

Security Fuses

There are three fuses on the device that must be blown during the device personalization process. Each fuse locks certain portions of the configuration memory as OTP memory. Fuses are designed for the module manufacturer, card manufacturer and card issuer and should be blown in sequence, although all programming of the device and blowing of the fuses may be performed at one final step.

Protocol Selection

The AT88SC0808C supports two different communication protocols.

- **Smart Card Applications**: The asynchronous T = 0 protocol defined by ISO 7816-3 is used for compatibility with the industry's standard smart card readers.
- **Embedded Applications**: A 2-wire serial interface is used for fast and efficient communication with logic or controllers.

The power-up sequence determines which of the two communication protocols will be used.

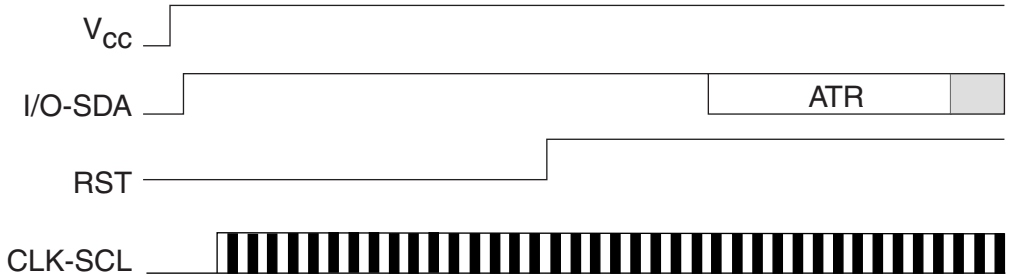
Asynchronous T = 0 Protocol

This power-up sequence complies with ISO 7816-3 for a cold reset in smart card applications.

- V_{CC} goes high; RST, I/O-SDA and CLK-SCL are low.
- Set I/O-SDA in receive mode.
- Provide a clock signal to CLK-SCL.
- RST goes high after 400 clock cycles.

The device will respond with a 64-bit ATR code, including historical bytes to indicate the memory density within the CryptoMemory family. Once the asynchronous mode has been selected, it is not possible to switch to the synchronous mode without powering off the device.

Figure 10. Asynchronous T = 0 Protocol (Gemplus Patent)

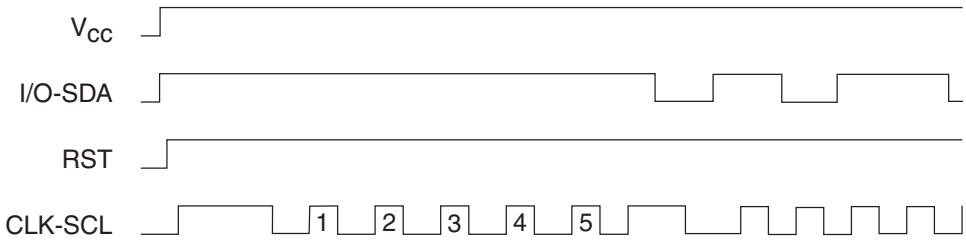


Synchronous 2-wire Serial Interface

The synchronous mode is the default after powering up V_{CC} due to an internal pull-up on RST. For embedded applications using CryptoMemory in standard plastic packages, this is the only communication protocol.

- Power-up V_{CC}, RST goes high also.
- After stable V_{CC}, CLK-SCL and I/O-SDA may be driven.

Figure 11. Synchronous 2-wire Protocol



Note: Five clock pulses must be sent before the first command is issued.

Communication Security Modes

Communications between the device and host operate in three basic modes. Standard mode is the default mode for the device after power-up. Authentication mode is activated by a successful authentication sequence. Encryption mode is activated by a successful encryption activation following a successful authentication.

Table 4. Communication Security Modes[1]

Mode	Configuration Data	User Data	Passwords	Data Integrity Check
Standard	Clear	Clear	Clear	MDC
Authentication	Clear	Clear	Encrypted	MAC
Encryption	Clear	Encrypted	Encrypted	MAC

Note: 1. Configuration data include viewable areas of the Configuration Zone except the passwords:
MDC: Modification Detection Code.
MAC: Message Authentication Code.

Security Options

Anti-tearing

In the event of a power loss during a write cycle, the integrity of the device's stored data may be recovered. This function is optional: the host may choose to activate the anti-tearing function, depending on application requirements. When anti-tearing is active, write commands take longer to execute, since more write cycles are required to complete them, and data are limited to eight bytes.

Data are written first to a buffer zone in EEPROM instead of the intended destination address, but with the same access conditions. The data are then written in the required location. If this second write cycle is interrupted due to a power loss, the device will automatically recover the data from the system buffer zone at the next power-up.

In 2-wire mode, the host is required to perform ACK polling for up to 8 ms after write commands when anti-tearing is active. At power-up, the host is required to perform ACK polling, in some cases for up to 2 ms, in the event that the device needs to carry out the data recovery process.

Write Lock

If a user zone is configured in the write lock mode, the lowest address byte of an 8-byte page constitutes a write access byte for the bytes of that page.

Example: The write lock byte at $080 controls the bytes from $080 to $087.

Figure 12. Write Lock Example

Address	$0	$1	$2	$3	$4	$5	$6	$7
$080	11011001	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx
		locked	locked			locked		

The write lock byte may also be locked by writing its least significant (rightmost) bit to "0". Moreover, when write lock mode is activated, the write lock byte can only be programmed – that is, bits written to "0" cannot return to "1".

In the write lock configuration, only one byte can be written at a time. Even if several bytes are received, only the first byte will be taken into account by the device.

Password Verification

Passwords may be used to protect read and/or write access of any user zone. When a valid password is presented, it is memorized and active until power is turned off, unless a new password is presented or RST becomes active. There are eight password sets that may be used to protect any user zone. Only one password is active at a time, but write passwords give read access also.

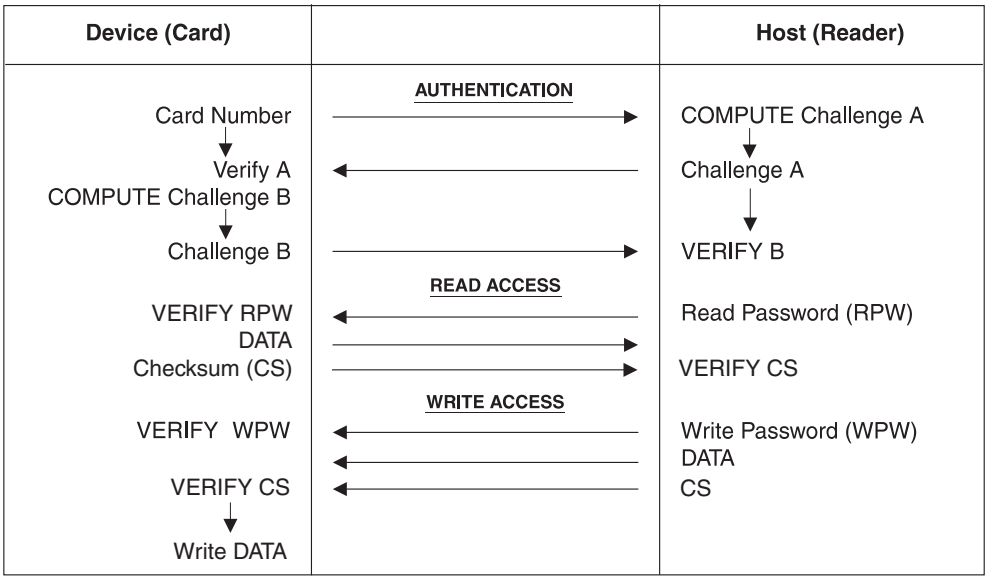
Authentication Protocol

The access to a user zone may be protected by an authentication protocol. Any one of four keys may be selected to use with a user zone.

The authentication success is memorized and active as long as the chip is powered, unless a new authentication is initialized or RST becomes active. If the new authentication request is not validated, the card loses its previous authentication and it should be presented again. Only the last request is memorized.

Note: Password and authentication may be presented at any time and in any order. If the trials limit has been reached (after four consecutive incorrect attempts), the password verification or authentication process will not be taken into account.

Figure 13. Password and Authentication Operations



Checksum

The AT88SC0808C implements a data validity check function in the form of a checksum, which may function in standard, authentication or encryption modes.

In the standard mode, the checksum is implemented as a Modification Detection Code (MDC), in which the host may read an MDC from the device in order to verify that the data sent was received correctly.

In the authentication and encryption modes, the checksum becomes more powerful since it provides a bidirectional data integrity check and data origin authentication capability in the form of a Message Authentication Code (MAC). Only the host/device that carried out a valid authentication is capable of computing a valid MAC. While operating in the authentication or encryption modes, the use of a MAC is required. For an ingoing command, if the device calculates a MAC different from the MAC transmitted by the host, not only is the command abandoned but the mode is also reset. A new authentication and/or encryption activation will be required to reactivate the MAC.

Encryption

The data exchanged between the device and the host during read, write and verify password commands may be encrypted to ensure data confidentiality.

The issuer may choose to require encryption for a user zone by settings made in the configuration memory. Any one of four keys may be selected for use with a user zone. In this case, activation of the encryption mode is required in order to read/write data in the zone and only encrypted data will be transmitted. Even if not required, the host may elect to activate encryption provided the proper keys are known.

Supervisor Mode

Enabling this feature allows the holder of one specific password to gain full access to all eight password sets, including the ability to change passwords.

Modify Forbidden

No write access is allowed in a user zone protected with this feature at any time. The user zone must be written during device personalization prior to blowing the security fuses.

Program Only

For a user zone protected by this feature, data within the zone may be changed from a “1” to a “0”, but never from a “0” to a “1”.

Initial Device Programming

To enable the security features of CryptoMemory, the device must first be personalized to set up several registers and load in the appropriate passwords and keys. This is accomplished through programming the configuration memory of CryptoMemory using simple write and read commands. To gain access to the configuration memory, the secure code must first be successfully presented. For the AT88SC0808C device, the secure code is $22 E8 3F. After writing and verifying data in the configuration memory, the security fuses must be blown to lock this information in the device. For additional information on personalizing CryptoMemory, please see the application notes *Programming CryptoMemory for Embedded Applications* and *Initializing CryptoMemory for Smart Card Applications* (at www.Atmel.com).

Ordering Information

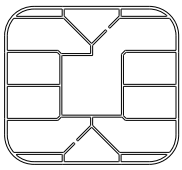
Ordering Code	Package	Voltage Range	Temperature Range
AT88SC0808C-MJ AT88SC0808C-MP	M2 – J Module M2 – P Module	2.7V–5.5V	Commercial (0°C–70°C)
AT88SC0808C-PU AT88SC0808C-SU	8P3 8S1	2.7V–5.5V	Green compliant (exceeds RoHS)/Industrial (–40°C–85°C)
AT88SC0808C-WI	7 mil wafer	2.7V–5.5V	Industrial (–40°C–85°C)

Package Type[1]	Description
M2 – J Module	M2 ISO 7816 Smart Card Module
M2 – P Module	M2 ISO 7816 Smart Card Module with Atmel® Logo
8P3	8-lead, 0.300” Wide, Plastic Dual Inline Package (PDIP)
8S1	8-lead, 0.150” Wide, Plastic Gull Wing Small Outline Package (JEDEC SOIC)

Note: 1. Formal drawings may be obtained from an Atmel sales office.

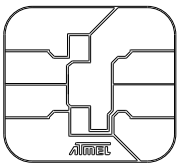
Packaging Information

Ordering Code: MJ



Module Size: **M2**
Dimension*: 12.6 x 11.4 [mm]
Glob Top: Round - ∅ 8.5 [mm]
Thickness: 0.58 [mm]
Pitch: 14.25 mm

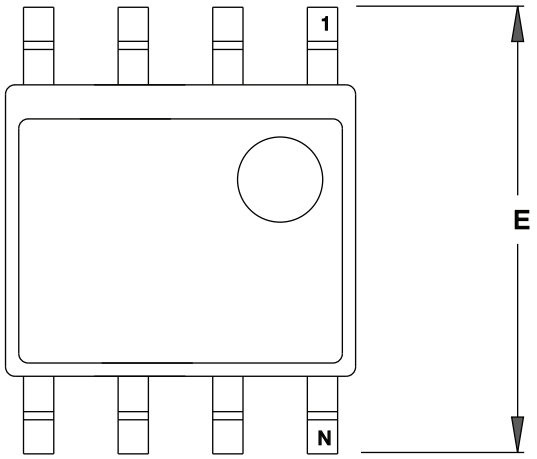
Ordering Code: MP



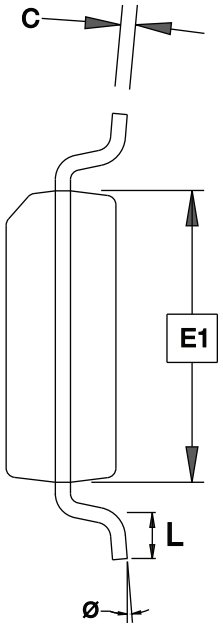
Module Size: **M2**
Dimension*: 12.6 x 11.4 [mm]
Glob Top: Square - 8.8 x 8.8 [mm]
Thickness: 0.58 [mm]
Pitch: 14.25 mm

*Note: The module dimensions listed refer to the dimensions of the exposed metal contact area. The actual dimensions of the module after excise or punching from the carrier tape are generally 0.4 mm greater in both directions (i.e., a punched M2 module will yield 13.0 x 11.8 mm).

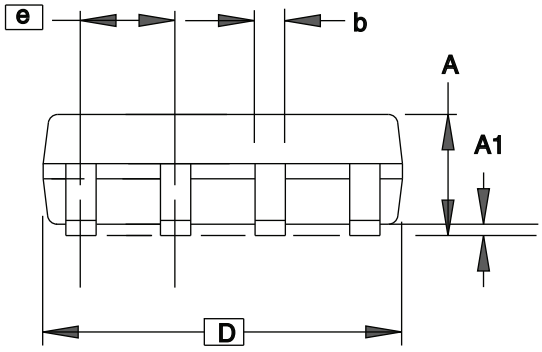
Ordering Code: SU
8-lead SOIC



TOP VIEW



END VIEW



SIDE VIEW

COMMON DIMENSIONS
(Unit of Measure = mm)

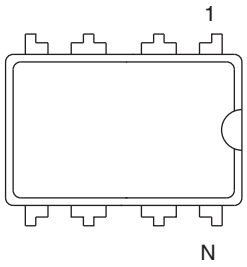
SYMBOL	MIN	NOM	MAX	NOTE
A	1.35	–	1.75	
A1	0.10	–	0.25	
b	0.31	–	0.51	
C	0.17	–	0.25	
D	4.80	–	5.05	
E1	3.81	–	3.99	
E	5.79	–	6.20	
e	1.27 BSC			
L	0.40	–	1.27	
θ	0°	–	8°	

Note: These drawings are for general information only. Refer to JEDEC Drawing MS-012, Variation AA for proper dimensions, tolerances, datums, etc.

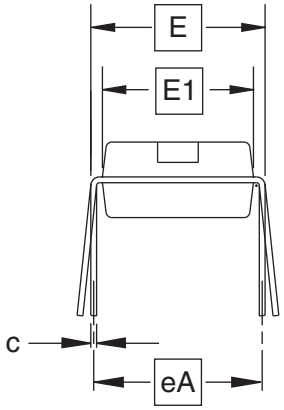
3/17/05

1150 E. Cheyenne Mtn. Blvd. Colorado Springs, CO 80906	**TITLE** **8S1**, 8-lead (0.150" Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)	**DRAWING NO.** 8S1	**REV.** C

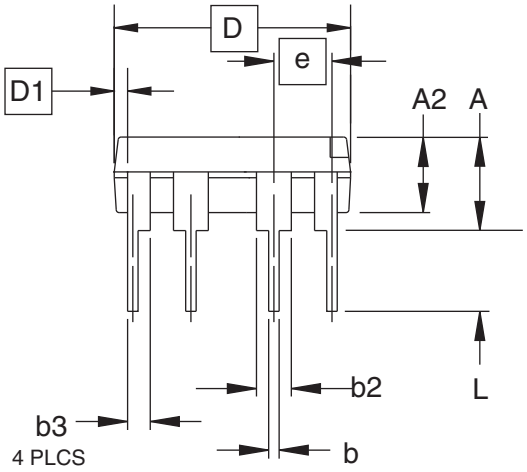
Ordering Code: PU
8-lead PDIP



Top View



End View



Side View

COMMON DIMENSIONS
(Unit of Measure = inches)

SYMBOL	MIN	NOM	MAX	NOTE
A			0.210	2
A2	0.115	0.130	0.195	
b	0.014	0.018	0.022	5
b2	0.045	0.060	0.070	6
b3	0.030	0.039	0.045	6
c	0.008	0.010	0.014	
D	0.355	0.365	0.400	3
D1	0.005			3
E	0.300	0.310	0.325	4
E1	0.240	0.250	0.280	3
e	0.100 BSC			
eA	0.300 BSC			4
L	0.115	0.130	0.150	2

Notes:
1. This drawing is for general information only; refer to JEDEC Drawing MS-001, Variation BA for additional information.
2. Dimensions A and L are measured with the package seated in JEDEC seating plane Gauge GS-3.
3. D, D1 and E1 dimensions do not include mold Flash or protrusions. Mold Flash or protrusions shall not exceed 0.010 inch.
4. E and eA measured with the leads constrained to be perpendicular to datum.
5. Pointed or rounded lead tips are preferred to ease insertion.
6. b2 and b3 maximum dimensions do not include Dambar protrusions. Dambar protrusions shall not exceed 0.010 (0.25 mm).

01/09/02

	TITLE	DRAWING NO.	REV.
2325 Orchard Parkway San Jose, CA 95131	**8P3**, 8-lead, 0.300" Wide Body, Plastic Dual In-line Package (PDIP)	8P3	B

Revision History

Doc. Rev.	Date	Comments
2024JS	3/2009	Features Section – add ‘Green compliant (exceeds RoHS) to end of ‘Standard 8-lead Plastic Packages’ bullet added Note to DC Characteristics table and applied to Vcc and all 3 instances of Vih symbols in table. Ordering Information page: Add ‘Green compliant (exceeds RoHS) to middle row of Temperature Range Replace ‘Lead-free/Halogen-free. Keep industrial Updated to 2009 Copyright.
2024IS	11/2008	Updated timing diagrams.
2024HS	4/07	Final release version
2024HS	1/25/07	Replaced User Zone, Configuration Memory, and Write Lock Example tables with new information
2024HS	1/2007	Implemented revision history. Removed Industrial package offerings. Removed 8Y4 package offering.